Accuracy

BLOCKCHAIN EPISODE 1 - BLOCKCHAIN TECHNOLOGY IS BRINGING ABOUT THE REMODELLING OF ECONOMIC LIFE

TECH

SEPTEMBER 2018 | 11 MINUTE READ

Nicolas Darbo
Partner

Martin Della Chiesa
Manager

Clément Téqui
Associate

Blockchain technology is effecting fundamental change in the structure and organisation of economic life. We can appreciate and understand its impact through an analogy between blockchain and the internet. When the internet first appeared, it allowed a number of new players to emerge, such as the GAFA[1] companies. Their economic models are almost entirely internet-based, making them *pure players*. Nevertheless, we cannot limit the impact of the internet to the creation of these companies: each business in the traditional economy has been able to use the internet to create new functions (e.g. online orders) or improve internal processes (e.g. reduction of communication costs thanks to videoconferencing).

Blockchain technology can therefore have as much of an impact on economic life as the internet: on one hand, pure players will emerge whose economic models will be entirely based on the technology; on the other hand, traditional businesses will be able to develop new functions and improve internal processes.

[1] *Google, Amazon, Facebook and Apple*

The blockchain ecosystem is structured around two axes: the level of decentralisation and the complexity of use cases.

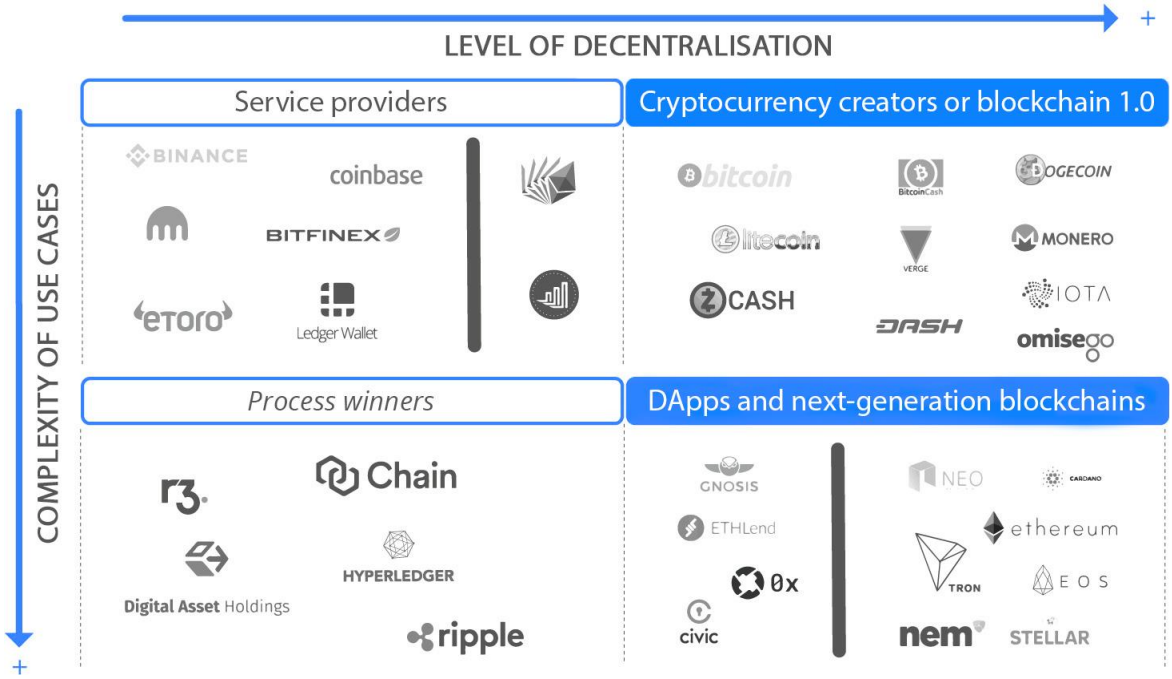
- The horizontal axis measures the level of decentralisation of the organisation, facilitating the distinction between centralised and more decentralised players. The most centralised players are those who use permissioned or private blockchains as well as those gravitating around the blockchain ecosystem without using its technology. The most decentralised players are those using public blockchains[2].

- The vertical axis measures the complexity of the use cases of the proposed product, thus facilitating the distinction between upstream and downstream players in the ecosystem's value chain, with the breaking point between the upstream and downstream players being the use (or not) of Smart Contracts.

We are able to map out four types of player when combining these axes:

- **Service providers**
- **Process winners**
- **Cryptocurrency creators or Blockchain 1.0**
- **DApps or Blockchain 2.0.**

Mapping of players in their ecosystem



[2] *In reality, all players using public blockchains do not have the same level of decentralisation. In fact, a business's level of decentralisation in the blockchain ecosystem is essentially defined by the role played by the token in its economic model. A high level of decentralisation implies a token which guarantees a maximum alignment of interest within the created ecosystem, in the absence of direct intervention from a centralised third party. In contrast, a lower level of decentralisation is explained by the intervention of a centralised player in the circulation of crypto-assets. Contrary to popular misconceptions, the direct link between new players in the blockchain ecosystem and decentralisation is far from automatic.*

1. SERVICE PROVIDERS

Generally speaking, these players can be compared to the sellers of shovels during the Gold Rush.
The service provider category groups those who propose a service or product linked to the blockchain ecosystem. These players tend to be rather centralised, as they follow a traditional organisation and are situated upstream in the value chain according the previously defined differentiation criteria. They are considered service providers that facilitate the appropriation and penetration of the technology because they participate directly in the development and securitisation of the ecosystem. In this category, we distinguish between four sub-categories: advisors, exchangers, regulators and storage services.

2. PROCESS WINNERS

Process Winners are those who consider blockchain technology as a means of improving internal processes in traditional-economy businesses through increased automaticity, transparency and security. This can provide two levers for growth: an increase in revenues and a decrease in costs. Amongst these initiatives, some are led by traditional-economy players who wish to appropriate blockchain technology via investments in research and development, partnerships or acquisitions, whilst others are led by start-ups in the blockchain ecosystem.

3. DAPPS AND NEXT-GENERATION BLOCKCHAINS

The crypto-apps category is larger and more complex than that of cryptocurrency creators; indeed, it groups downstream players in the value chain who provide services that far exceed the purely monetary. They carry the seeds of radical change in the economic paradigm. Blockchain technology has opened the way to token economics where a business can offer a service and a cryptocurrency to pay for that service. It consequently becomes both a traditional-economy business whose economic model is based on the product or service sold and, at the same time, a central bank issuing its own currency.
This system therefore distinguishes between, on one hand, the players providing infrastructure to the crypto-apps (Chain Producers) and, on the other, those using this infrastructure to develop applications and uses (Chain Users).

4. CRYPTOCURRENCY CREATORS OR BLOCKCHAIN 1.0

Cryptocurrency creators or Blockchain 1.0 are those who have developed decentralised protocols based on blockchain's technological layers furthest upstream in terms of the value chain and innovation: the ledger and transaction layers. They enable the use of blockchain technology with a sole focus on currency. Cryptocurrency creators group together players that have developed cryptocurrencies competing more or less directly with Bitcoin, the leader in this category. It is worth noting that cryptocurrency projects were, in fact, the first to appear chronologically[3].

[3] The IOTA project appeared later than the others but offers a particular use case for its cryptocurrency as it is centred solely on connected objects.

To map this category, we propose two axes of analysis.

The first (i.e. the horizontal axis) is transaction speed: the higher a currency's transaction speed, the more it can replace fiat currencies, whose transaction speed is, in practice, instantaneous. Indeed, it is difficult to imagine the widespread adoption of cryptocurrencies as a means of payment for micro-transactions if it takes 10 minutes to validate a transaction, as is currently the case for Bitcoin. To improve the transaction speed of a cryptocurrency, various possibilities exist:

- reducing the validation time of blocks;
- increasing the size of blocks and therefore the number of transactions each block can register;
- modifying/lightening the validation protocol.

In what follows, the volume of transactions – or scalability – refers to the number of transactions per second[4] that can be compared with current means of payment (e.g. Visa – able to cover several thousand transactions per second). Before detailing the solutions which could improve transaction speed, we highlight the virtually inevitable compromise between speed and security, resulting from the way in which cryptocurrencies have been constructed. In the case of Bitcoin, its security derives from the fact that its consensus algorithm – its proof of work – allows an almost infinite level of security, where the alteration of historical data is impossible. This security is guaranteed by the validation time of approximately 10 minutes chosen by its creator. If we were to reduce this validation time, security would suffer as it would be easier to modify the transaction history. To overcome this compromise, certain projects are trying to create new validation processes.

The second axis (i.e. the vertical one) is the level of confidentiality: currencies with absolute confidentiality will not necessarily serve the same purposes as those with a lower level of it. These currencies with a lower level of confidentiality, or pseudo-anonymous currencies, are those where the quantity associated with each wallet is known, but the identity of the owner is not, as is the case with Bitcoin, for example. This type of currency offers a usage similar to that of bank account management where money is exchanged via transfers[5].
Currencies with a significant level of confidentiality, or perfectly anonymous currencies, are those where neither the amount associated with each wallet nor the identity of its owner is known. This type of currency offers a usage similar to that of cash and is more suited to micropayments. As these currencies centre on the notion of cash and anonymity, their susceptibility to being used in certain illegal transactions such as the purchase of arms or drugs cannot be denied.

The combination of these two axes results in the following three categories that we will go on to detail further:

- Bitcoin and its fellows
- Secret money (confidential solutions)
- High-tech money (next-generation solutions)

[4] The notion of the number of transactions per second should not be confused with that of the instantaneity of transactions.
[5] This could be used by commercial businesses which undertake regular significant transfers requiring a maximum level of security.

I. BITCOIN AND ITS FELLOWS

As Bitcoin was the first cryptocurrency, its technology presents certain limitations that other projects have tried to overcome. Bitcoin's source code is open source, that is, completely free to access online. The projects in this category start from this source code and marginally modify its settings. In this respect, we can say that "code is business", given that the code is adapted to fulfil a market need. The primary modifications relate to validation time and block size, and amongst the most well-known of these projects, we discuss Litecoin, Bitcoin Cash and Dogecoin below.

The validation time of a block under the Bitcoin protocol is approximately ten minutes. If we equate this validation time per block to transactions, we estimate that the Bitcoin protocol is able to validate approximately three transactions per second, compared with 2,500 for Visa. In order to validate more quickly, the Litecoin protocol, which is based on the Bitcoin protocol, offers block validation approximately every 2.5 minutes[6]. As for the Dogecoin protocol, it offers block validation approximately every minute. Dogecoin's aim is consequently to become the currency of tips on the Internet: a user who liked a video or a tweet could leave some Dogecoins, the value of which is mostly symbolical[7]. The Dogecoin project was originally a joke, aiming to show how easy it is to create a cryptocurrency starting from the Bitcoin source code. This joke was nonetheless well received by the blockchain community.

Bitcoin's creators fixed the maximum size of a block able to be validated under the Bitcoin protocol at 1 MB. This limitation could result in the network becoming saturated, which would lead to a longer transaction time. Network miners have long debated increasing the maximum size of a block, but as those for and those against were unable to find a common position, they created a hard fork in August 2017. It gave rise to the creation of the Bitcoin Cash protocol, which allows a maximum block size able to be validated of 8 MB. It is interesting to note that, until the date of the separation (1 August 2017), the two protocols had the same transaction history[8].

II. SECRET MONEY

The completely anonymous currencies fulfil a need not yet addressed by cryptocurrencies: digital cash[9]. They also take inspiration from the Bitcoin source code but change its philosophy more radically by including the notion of pure anonymity. Amongst the most well-known of them, we discuss Dash, Zcash, Monero and Verge below. Although the degrees of confidentiality offered are well matched to illegal transactions, and notably the dark web, in reality these cryptocurrencies go far beyond this context.

The Bitcoin protocol guarantees a certain level of confidentiality to its users thanks to the existence of private and public keys. However, it was created so that, via the public key, a user could access the transaction register and discover the origin, the amount and the recipient of funds transferred. This is the very principle of the Bitcoin protocol: to be a distributed register where anyone at any time can consult the entire history of transactions.
The Dash protocol aims to be a digital equivalent to cash[10]. To this end, its creator, Evan Duffield, imagined two technologies superimposed on the Bitcoin protocol: InstantSend, which offers immediate transactions, and PrivateSend, which offers fully confidential transactions for users who want them[11].

---

[6] https://litecoin.org/fr/
[7] http://dogecoin.com/. Dogecoin is represented by the head of a Shiba Inu, something very popular in Internet communities.
[8] https://www.bitcoincash.org/
[9] This statement can seem contradictory in light of the title of Bitcoin's White Paper A Peer-to-Peer Electronic Cash System. However, for the reasons detailed previously, we believe that the usage of Bitcoin cannot be considered similar to digital cash.
[10] https://github.com/dashpay/dash/wiki/Whitepaper
[11] https://www.dash.org/

The Zcash protocol offers a currency where transaction anonymity is absolute, thanks to the concept of 'zero knowledge proof'. In this way, by using Zcash, a user can choose to hide the origin, amount and recipient of the transaction. Nevertheless, thanks to zero knowledge proof, the Zcash protocol is able to guarantee that the transaction took place without providing information about it (origin, destination and amount).

The Bytecoin protocol is based on CryptoNote technology. It is therefore not a Bitcoin fork but a newly created blockchain. The advantage of CryptoNote technology is the ability to offer a high level of confidentiality as well as a transaction time of approximately two minutes[12]. A number of other currencies have been developed from Bytecoin forks, such as Monero (which modifies characteristics to increase mining speed and uses a 'one-time' technique for public addresses thus rendering it impossible to trace the balance of an account)[13].

Verge offers 'protection of our digital privacy' thanks to the use of multiple networks focussed on anonymity, such as Tor and i2p where users' IP addresses are completely hidden and, consequently, transactions are untraceable.

III. HIGH-TECH MONEY

High-tech currencies aim to go beyond the Bitcoin protocol quite significantly. They offer new uses for cryptocurrencies all while bringing technological answers to the primary criticisms and/or limitations of Bitcoin, namely:

- its lack of scalability;
- its transaction fees, which can be high;
- its energy consumption issues linked to proof of work.

We will discuss the most well-known of these high-tech currencies: Iota, Nano and OmiseGO.

Iota, in terms of technology, is a fundamentally different currency from the Bitcoin protocol. Indeed, it aims to do without blocks – something essential to blockchain technology – by using dispersed validation nodes. It is a currency that applies to connected objects, the idea being to make available the small amount of calculation power embedded in each connected object to validate transactions, thus combining the notion of miner and network user. Consequently, it is no longer necessary to concatenate transactions in a block to validate them. This mechanism is called *Tangle*, and it relies on a Directed Acyclic Graph to register the transactions[14].

Nano, formerly known as Railblock, is similar to Iota in the sense that the concepts of miner and user are more or less combined[15]. However, it does not apply to connected objects. Its use case concentrates on maximum efficiency around transactions: they are validated in two seconds, without transaction fees and with unlimited scalability[16].

OmiseGO is a particular currency which relies on the Ethereum blockchain to be deployed and can be, in this sense, likened to a crypto-app. We have chosen to classify it in the cryptocurrency category, however, as its use case is essentially centred on payments from applications or Internet sites. OmiseGO offers currency storage and transfer technology in real time, and it is indifferent to jurisdictions, organisations or the type of currency dealt with, be it traditional or cryptocurrency. The OmiseGO token is not a medium of exchange, in contrast to

---

[12] https://bytecoin.org/

[13] http://whitepaperdatabase.com/monero-xmr-whitepaper/

[14] This concept is highly technical and requires a certain mastery of mathematics to be able to understand it fully. It was formalised by Sergei Popov, a renowned mathematician from the University of Campinas in Brazil and an active member of the cryptocurrency community. The formalisation is accessible via the following link: https://iota.org/IOTA_Whitepaper.pdf

[15] Iota relies on Tangle for this mechanism, whilst Nano relies on the 'block lattice' mechanism, which nonetheless retains the principle of the implementation of a directed acyclic graph.

[16] https://nano.org/en/whitepaper

the currencies mentioned previously, but it is used to validate transactions and allows a user to obtain discounts and/or rewards when used to make a payment.

CONCLUSION

In conclusion, the cryptocurrency category groups players who have developed cryptocurrencies for purely monetary purposes. They have often created initiatives deviating slightly from the Bitcoin source code by incorporating slight modifications without fundamentally changing the product offered, even if some cryptocurrencies have been created with more significant changes to the protocols, such as Zcash or Bytecoin.

The result? Today, we count more than 30 cryptocurrencies with purely monetary use cases. We have limited our examples to those with the highest market capitalisation (as at the end of 2017). As explained previously, it cannot be denied that cryptocurrencies have given rise – almost ex nihilo – to a large number of competing currencies with low long-term viability. They provide, nonetheless, an example of Hayek's theory on competing currencies: the selection of good and bad currencies will be made, in the long term, by consumer choice.

The cryptocurrencies discussed previously can be broken down as shown in the following graph. The size of the bubbles represents market capitalisation, calculated as the number of coins in circulation multiplied by the unit price using data as at 31 December 2017. The transactions are expressed in transactions per second with a logarithmic scale.

Breakdown of currencies according to their level of confidentiality and transaction speed